



250-561^{Q&As}

Endpoint Security Complete - Administration R1

Pass Symantec 250-561 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/250-561.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Which framework, open and available to any administrator, is utilized to categorize adversarial tactics and for each phase of a cyber attack?

- A. MITRE RESPONSE
- B. MITRE ATTandCK
- C. MITRE ADVandNCE
- D. MITRE ATTACK MATRIX

Correct Answer: C

QUESTION 2

Which two (2) skill areas are critical to the success of incident Response Teams (Select two)

- A. Project Management
- B. Incident Management
- C. Cyber Intelligence
- D. Incident Response
- E. Threat Analysis

Correct Answer: CD

QUESTION 3

Which file should an administrator create, resulting Group Policy Object (GPO)?

- A. Symantec__Agent_package_x64.zip
- B. Symantec__Agent_package_x64.msi
- C. Symantec__Agent_package__32-bit.msi
- D. Symantec__Agent_package_x64.exe

Correct Answer: C

QUESTION 4

What are the Exploit Mitigation security control's mitigation techniques designed to prevent?



- A. Packed file execution
- B. Misbehaving applications
- C. File-less attacks
- D. Rootkit downloads

Correct Answer: D

QUESTION 5

What are two (2) benefits of a fully cloud managed endpoint protection solution? (Select two)

- A. Increased content update frequency
- B. Increased visibility
- C. Reduced 3rd party licensing cost
- D. Reduced database usage
- E. Reduced network usage

Correct Answer: CD

[Latest 250-561 Dumps](#)

[250-561 Study Guide](#)

[250-561 Exam Questions](#)